A Blind Watermarking Technique using Redundant Wavelet Transform for Copyright Protection

Ferda Ernawan
Faculty of Computer Systems & Software Engineering,
Universiti Malaysia Pahang
Kuantan, Malaysia
e-mail: ferda@ump.edu.my

Muhammad Nomani Kabir
Faculty of Computer Systems & Software Engineering,
Universiti Malaysia Pahang
Kuantan, Malaysia
e-mail: nomanikabir@ump.edu.my

***Abstract*— A digital watermarking technique is an alternative method to protect the intellectual property of digital images. This paper presents a hybrid blind watermarking technique formulated by combining RDWT with SVD considering a trade-off between imperceptibility and robustness. Watermark embedding locations are determined using a modified entropy of the host image. Watermark embedding is employed by examining the orthogonal matrix *U* obtained from the hybrid scheme RDWT-SVD. In the proposed scheme, the watermark image in binary format is scrambled by Arnold chaotic map to provide extra security. Our scheme is tested under different types of signal processing and geometrical attacks. The test results demonstrate that the proposed scheme provides higher robustness and less distortion than other existing schemes in withstanding JPEG2000 compression, cropping, scaling and other noises.**

Keywords—blind watermarking technique; modified entropy; watermark insertion; watermark extraction; redundant wavelet transform

I. INTRODUCTION

With the advancement of technology, transmission and distribution of digital multimedia data (image, audio, video, etc.) become vulnerable to unauthorized duplication. Therefore, now-a-days watermarking techniques that can verify the authenticity of the digital data are important to protect the intellectual properties or copyrights in digital images [1]-[3]. Some essential features of image watermarking are invisibility, robustness and security. The technology of digital watermarking has recently attracted to improve the robustness against several types of attacks.

Many watermarking schemes have been presented using frequency domain and singular value decomposition (SVD) [5]-[8]. Makbol-Khoo [9] presented an embedding scheme that directly inserts the watermark into the singular values *S* obtained from redundant wavelet transform (RDWT)-SVD. Ling et al. [10] verified the flaw of false-positive problem in Makbol-Khoo scheme in the recovered watermark. Ling et al. [10] revealed that Makbol-Khoo scheme is dependent on the watermark's U_w and V_w orthogonal matrices.

In 2016, Makbol et al. [11] adopted another embedding technique derived from Lai scheme [12], where a watermark is inserted by examining the 1st column of *U* obtained from the hybrid DCT-SVD scheme. Furthermore, the authors presented block-based DWT-SVD based on HVS characteristics [11], while their scheme provides drawbacks of the down-sampling of its bands. The shift variance of DWT produces inaccuracy in watermark extraction [9]. They also provided a feature of encryption for selected block locations. Encrypted coordinates on the selected blocks provided weak security and confidentiality of the watermark image. It can be obtained by attacks by finding the significant information of the image. Furthermore, they used a threshold for watermark embedding in the orthogonal matrix *U* that resulted in an important issue due to invalid imperceptibility and robustness results. More crucially, the results in [11] were weak because the watermark embedding uses the same threshold for different hybrid schemes (e.g. DCT-SVD and DWT-SVD). A threshold cannot be used for different hybrid schemes and it must consider a balance between imperceptibility and robustness of watermarked images.

This paper presents a 4×4 RDWT-SVD image watermarking technique based on modified entropy considering an optimal threshold value. Arnold chaotic map is used to scramble the watermark image for improving security and confidentiality of the watermarked image. The scrambled binary watermark is embedded by modifying $U_{3,1}$ and $U_{4,1}$ coefficients of the orthogonal matrix *U* obtained from RDWT-SVD using specific rules. The robustness of watermarked images is measured under different types of geometric and signal processing attacks. The proposed scheme is designed to reduce the possibility of the false-positive problem in the extracted watermark. False-positive problems exhibited in Makbol-Khoo scheme [9], Zhang and Li [14], Rykaczewski [15], Liu-Tan [16] and Lai-Tsai [17].

II. METHOD AND MATERIALS

A. Arnold Scrambling

Arnold scrambling can improve the security of watermarked image [18][19]. Arnold scrambling transformation [20][21] is defined by:

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \bmod N \quad (1)$$

where $\begin{pmatrix} x' \\ y' \end{pmatrix}$ represents the vector position after shifting, $\begin{pmatrix} x \\ y \end{pmatrix}$ denotes the original vector position before shifting and *mod* stands for the modulus operation with the divisor *N*. The number of scrambling iterations is also given by *N*. In this paper, *N* is considered as a key. The inverse Arnold scrambling is defined by:

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} x' \\ y' \end{pmatrix} \bmod N \quad (2)$$

B. Modified Entropy

Entropy is measured by the spatial correlation of neighbour pixels and it carries important information of an image. Meanwhile, edge entropy provides important information of the image characteristics. The combination of these techniques indicates less distortion area of the image. Modified entropy is defined as follows:

$$E_{HVS} = -\sum_{i=1}^{N} (p_i \exp^{1-p_i} + p_i \log_2(p_i))/2 \quad (3)$$

where p_i denotes the occurrence probability of *i*-th pixel with $0 \le p_i \le 1$. The blocks with the lowest modified entropies are selected for embedding the watermark.

C. RDWT

RDWT eliminates up-sampling and down-sampling of coefficients which appear in DWT during filter-bank iterations [22]. Analysis and synthesis of RDWT can be presented by the following equations:

- RDWT Analysis:

$$k_j[i] = (k_{j+1}[i] * g_j[-i]), \quad (4)$$

$$l_j[i] = (k_{j+1}[i] * g_j[-i]) \quad (5)$$

- RDWT Synthesis:

$$k_{j+1}[i] = \frac{1}{2}(k_j[i] * h_j[i] + l_j[i] * g_j[i]) \quad (6)$$

where $h[-i]$ and $g[-i]$ refer to low-pass and high-pass analysis filters, respectively; $h[i]$ and $g[i]$ denote low-pass and high-pass synthesis filter; k_j and l_j represent low-band and high-band coefficients, respectively at level *j*. *LL* sub-band obtained from the selected block of RDWT coefficients is then decomposed by SVD.

D. Singular Value Decomposition(SVD)

SVD is a widely used in image-watermarking applications. In SVD, a matrix *A* is decomposed as

$$A = USV^T \quad (7)$$

where *S* is a diagonal matrix where diagonal entries are the squares (of the eigenvalues of *A*) arranged in lower order; and *U* and *V* are the orthonormal matrices.

III. PROPOSED SCHEME

A. Insertion Algorithms

The process of watermark insertion is described in Algorithm 1 and Fig. 1. A watermark image is embedded by examining the entries $U_{3,1}$ and $U_{4,1}$ of the 1st column of *U*. The relationship between these coefficients is considered to determine watermark bit of 0 or 1.

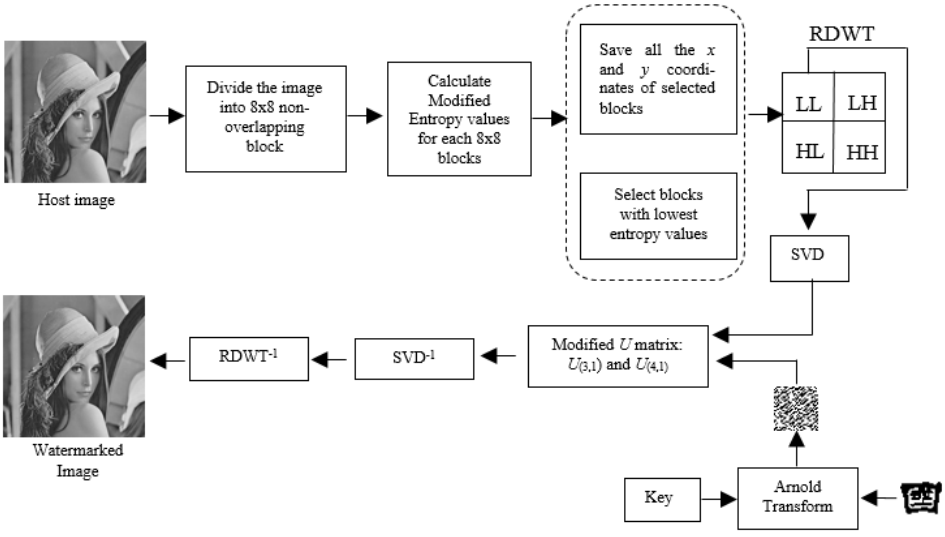


Fig. 1. Watermark insertion.

Algorithm 1: Insertion process

Input: Host image, watermark; T=0.055

Pre-processing:

Step 1: A host image is divided into 8×8 pixels.

Step 2: Compute a modified entropy for each non-overlapping block

Step 3: Select blocks that have lowest modified entropy values and save the location coordinates.

Step 4: A binary watermark is scrambled using Arnold chaotic using a secret key.

Watermark Insertion:

Step 5: Selected blocks are transformed using RDWT, the first level of LL sub-band coefficients is applied by SVD.

Step 6: The following rules are used to embed the watermark bits:

Rule 1: if the $U_{3,1}$ or $U_{4,1}$ coefficients are negative values, then x= -1, α= -T, otherwise if the $U_{3,1}$ or $U_{4,1}$ coefficients are positive, we set x= 1, α= T. Then, calculate the average $U_{3,1}$ and $U_{4,1}$ coefficients by: $m = \frac{|U_{3,1}| + |U_{4,1}|}{2}$

Rule 2: if the binary watermark bit =1,
$U_{3,1}=x\cdot m+\alpha/2$, $U_{4,1}=x\cdot m-\alpha/2$

Rule 3: if the binary watermark bit =0,
$U_{3,1}=x\cdot m-\alpha/2$, $U_{4,1}=x\cdot m+\alpha/2$

Post-processing after embedding:

Step 7: Apply the inverse SVD, then perform the inverse RDWT on each selected block.

Output: Watermarked image containing a logo

B. Extraction Algorithms

Steps of watermark extraction are given in Algorithm 2 and Fig. 2.

Algorithm 2: Extraction process

Input: Watermarked image; selected block locations

Pre-processing:

Step 1: The selected block locations are utilized to extract the watermark. Selected regions are split into 8×8 pixels.

Step 2: Apply the first level of RDWT on each selected block.

Step 3: Decompose LL sub-band of RDWT coefficients using SVD into U, S and V.

Watermark extraction:

Step 4: $U_{3,1}$ and $U_{4,1}$ coefficients are used to determine the watermark bits using a rule as follows:
If $|U_{3,1}|-|U_{4,1}|>0$, then set the watermark bit =1, else the watermark bit = 0.

Post-processing:

Step 5: After extraction process, apply the inverse Arnold transform using the same key to recover the watermark image.

Output: Watermark extraction

IV. Experimental Results

A binary watermark image with 32×32 pixels is shown in Fig. 3. Arnold transform is used to scramble the watermark image for improving the security and confidentiality of the watermark before insertion. Our scheme was tested on six benchmark images with 512×512 pixels, namely Lena, Sailboat, Pepper, Airplane, Lake and Baboon images as shown in Fig. 4. Tests include different types of simulated attacks using JPEG- and JPEG2000-compression, noise addition, filtering, adjust, histogram equalization, crop, rotation, translation and scaling. Comparison of performance of our watermarking scheme is made with an existing scheme.

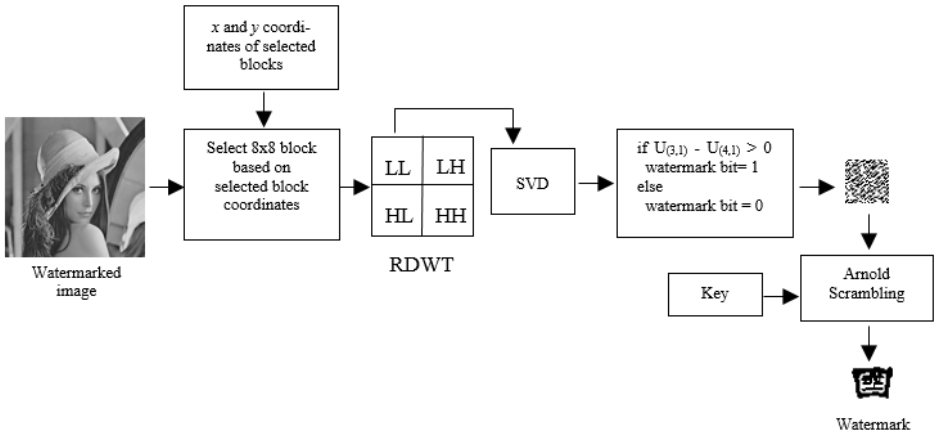
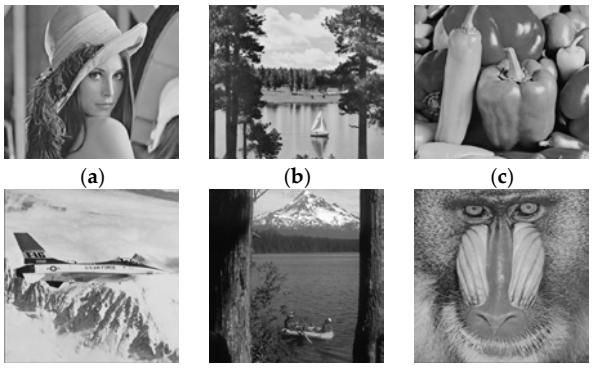


Fig. 2. Watermark extraction.

(a) (b)

Fig. 3. (a) A binary watermark 32×32 pixels, (b) The corresponding scrambled watermark.



(a) (b) (c)

(d) (e) (d)

Fig. 4. (a) Lena (b) Sailboat (c) Pepper (d) Airplane (e) Lake (f) Baboon.

A. Imperceptibility Measurement

The watermarked images quality is measured by PSNR and SSIM values. PSNR and SSIM measurements are used to evaluate the imperceptibility and the perceptual similarity of a watermarked image. The terms PSNR is defined as:

$$PSNR = 10\log_{10}\frac{255^2}{\frac{1}{MN}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}(g(x,y)-f(x,y))^2} \quad (8)$$

where g refers to the watermarked image and f represents the host image. The size of the watermarked image is given by $M \times N$. The term SSIM is defined by:

$$SSIM(x,y) = [l(x,y)]^{\alpha} \cdot [c(x,y)]^{\beta} \cdot [s(x,y)]^{\gamma} \quad (9)$$

where $\alpha>0$, $\beta>0$ and $\gamma>0$ are parameters which can be adjusted. A further description can be found in [23].

B. Robustness Measurement

Robustness properties of our scheme are evaluated by Normalized Cross-Correlation (NC) and Bit Error Rate (BER). Specifically, NC and BER are used to calculate the robustness of the recovered watermark after certain attack on the watermarked image occurs. NC and BER can be calculated by:

$$NC = \frac{\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}W(x,y).W^*(x,y)}{\sqrt{\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}W(x,y)^2\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}W^*(x,y)^2}} \quad (10)$$

$$BER = \frac{\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}W(x,y)\oplus W^*(x,y)}{M \times N} \quad (11)$$

where $\oplus$ represents exclusive OR operation. $W^*(x,y)$ denotes the watermark extraction and $W(x\ y)$ represents the binary watermark.

C. An optimal Threshold for Insertion

Watermark embedding is performed by examining the components: $U_{3,1}$ and $U_{4,1}$ of the orthogonal matrix U obtained from RDWT-SVD. Watermark bits are not directly inserted into U. By using some rules, the terms $U_{3,1}$ and $U_{4,1}$ are modified considering a threshold according to the scrambled watermark bits. An optimal threshold of Makbol scheme [11] and our scheme are shown in Figs. 5 and 6, respectively.

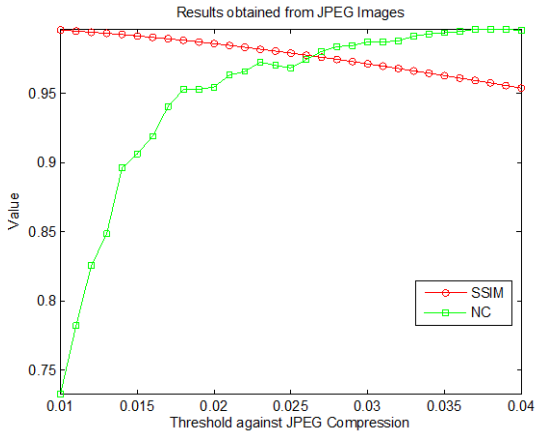


Fig. 5. An optimal threshold of Makbol scheme based on a trade-off between SSIM and NC values.

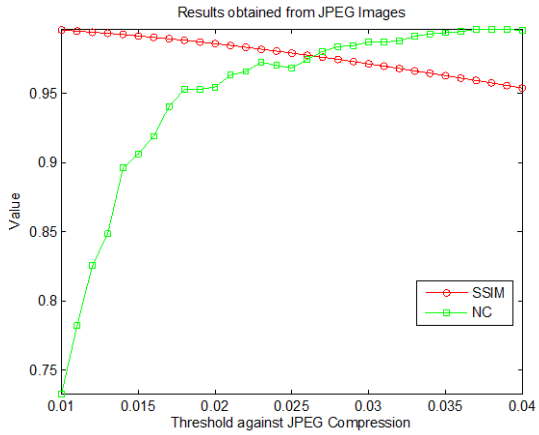


Fig. 6. An optimal threshold of Makbol scheme based on a trade-off between SSIM and NC values.

Using the experiment, we found an optimal threshold value as approximately 0.026 in the embedding process of Makbol scheme [11], while an optimal threshold for the proposed RDWT-SVD scheme as about 0.055. The threshold value was obtained by evaluating the trade-off between SSIM and NC values against JPEG compression. Image compression is extensively utilized for the reduction of amount of data as well as efficient transmission [24]-[25]. The experimental results of SSIM and NC values are provided in Table 1.

TABLE I. COMPARISON OF NC VALUES FROM EXTRACTED WATERMARK

Attack	Lena		Sailboat	
	Makbol [11]	Our scheme	Makbol [11]	Our scheme
No attack	1.0000	**1.0000**	**1.0000**	0.9942
Gaussian Low-pass filter [3 3]	0.9192	**0.9877**	0.9183	**0.9781**
Gaussian Low-pass filter [5 5]	0.4203	**0.9992**	0.4378	**0.9764**
Gaussian Noise 0.003	0.8652	**0.9347**	0.9292	**0.9598**
Gaussian Noise 0.03	0.6589	**0.7252**	0.6816	**0.7208**
Sharpening	1.0000	**1.0000**	**1.0000**	0.9926
Median Filter [3 3]	0.9496	**0.9992**	0.9434	**0.9859**
Median Filter [5 5]	0.0408	**0.7103**	0.2195	**0.7008**
Pepper and Salt 0.2%	**0.9925**	0.9867	**0.9925**	0.9858
Pepper and Salt 2%	0.8673	**0.8806**	**0.9066**	0.9038
Speckle Noise 0.03	0.7838	**0.8097**	0.7580	**0.7994**
Speckle Noise 0.3	0.5837	**0.6301**	**0.6037**	0.6029
Poisson Noise	0.9102	**0.9522**	0.9138	**0.9658**
Adjust	0.9975	**1.0000**	**0.9983**	0.9925
Histogram Equalization Attack	0.9899	**1.0000**	**0.9992**	0.9950
JPEG with *QF* =40	**0.9840**	0.9798	0.9823	**0.9875**
JPEG with *QF* =50	0.9747	**0.9942**	**0.9925**	0.9892
JPEG with *QF* =60	0.9925	**1.0000**	**0.9925**	0.9917

The proposed scheme produces less distortion and better perceptual quality than the existing schemes as demonstrated by PSNR and SSIM values in Table I. The watermarked images are tested under signal processing attacks. NC values of the extracted watermark after applying different geometric attacks are graphically depicted in Fig. 7. The test results demonstrate that our scheme produces higher robustness than Makbol scheme [11] as verified by NC values in Table II.

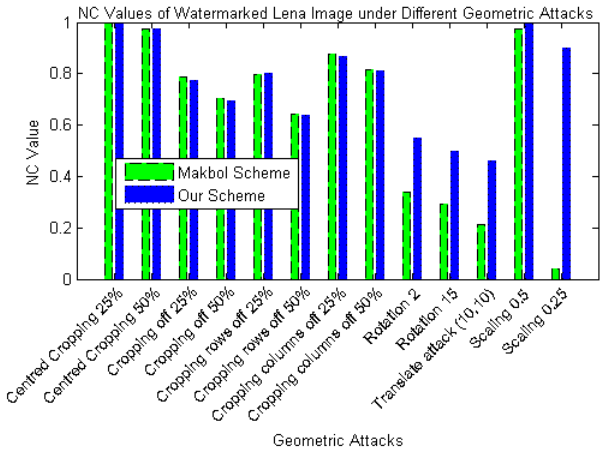


Fig. 7. Comparison of NC values under different types of geometric attack.

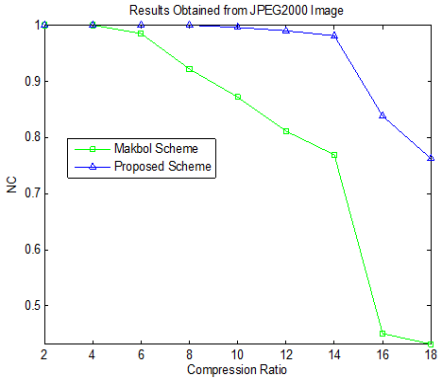


Fig. 8. Comparison of NC curves from Makbol scheme [11] and proposed scheme against JPEG2000 compression

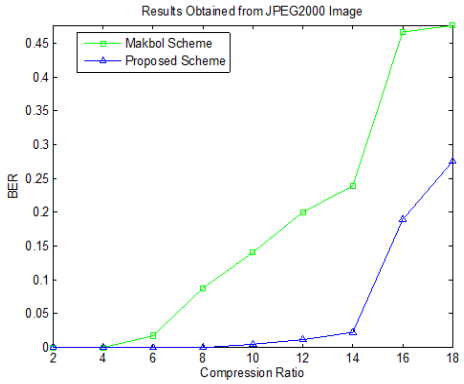


Fig. 9. Comparison of BER curves from Makbol scheme [11] and proposed scheme against JPEG2000 compression.

Figs. 8 and 9 show the comparison between Makbol scheme [11] and the proposed scheme considering compression with JPEG2000 under different compression ratios. The results prove that the proposed scheme can achieve higher robustness than Makbol scheme when the watermarked images are converted to JPEG2000 with a compression ratio more than 6. The proposed scheme also confirms superiority in robustness with JPEG2000 with different compression ratios as verified in NC and BER values.

TABLE II. COMPARISON OF VISUAL PERCEPTION FROM EXTRACTED WATERMARK

Attack	Lena		Sailboat	
	Makbol [10]	Our scheme	Makbol [10]	Our scheme
No attack				
Gaussian Low-pass Filter [3 3]				
Gaussian Low-pass Filter [5 5]				
Gaussian Noise 0.003				
Sharpening				
Median Filter [3 3]				
Pepper and Salt 0.2%				
Pepper and Salt 2%				
Speckle Noise 0.03				

Attack	Lena		Sailboat	
	Makbol [10]	Our scheme	Makbol [10]	Our scheme
Poisson Noise				
Adjust				
Histogram Equalization Attack				
JPEG with *QF* =50				

The proposed scheme produces stronger resistance and higher robustness than other existing schemes. Even the watermark extraction is damaged, the extracted watermark from the proposed scheme can still be observed by human visual systems.

V. CONCLUSION

This research presents a watermarking scheme using RDWT combined with SVD for protecting copyrights. Our scheme utilizes a modified entropy to determine the embedding regions with less distortion. A watermark image is scrambled by Arnold transform to provide extra security of the confidential information. The scrambled watermark is embedded in the host image by examining $U_{3,1}$ and $U_{4,1}$ coefficients obtained from RDWT-SVD used on the host image. Our scheme is tested against different types of signal processing and geometric attacks. Test results of our scheme show an improvement in terms of SSIM values and NC values compared to other existing schemes. The proposed scheme confirms satisfactory results, however, our scheme requires little higher computational cost due to Arnold transform and RDWT. It can be accepted because our aim is to improve the robustness against different types of attack.

ACKNOWLEDGMENT

The authors sincerely thank Universiti Malaysia Pahang, Malaysia for supporting this research work through UMP Research Grant Scheme (RDU170399).

REFERENCES

[1] N.A. Abu, F. Ernawan, N. Suryana, Sahib S, "Image watermarking using psychovisual threshold over the edge," *Information and Communication Technology, ICT-EurAsia,* vol. 7804, pp. 519-527, 2013.

[2] F. Ernawan, "Robust image watermarking based on psychovisual threshold," *Journal of ICT Research and Applications*, vol. 10, no. 3, pp. 228-242, 2016.

[3] F. Ernawan, M.N. Kabir, M. Fadli and Z Mustaffa, "Block-based Tchebichef image watermarking scheme using psychovisual threshold," *International Conference on Science and Technology-Computer* (ICST 2016), 2016, pp. 6-10.

[4] F. Ernawan, M. Ramalingam, A. S. Sadiq, Z. Mustaffa, "An improved imperceptibility and robustness of 4x4 DCT-SVD image watermarking using modified entropy," *Journal of Telecommunication, Electronic and Computer Engineering*, vol. 9, no. 2-7, pp. 111-116, 2017.

[5] I.A. Ansari, M Pant, "Multipurpose image watermarking in the domain of DWT based on SVD and ABC," *Pattern Recognition Letters*, vol. 94, pp. 228-236, 2017.

[6] S. Fazli, M. Moeini, "A robust image watermarking method based on DWT, DCT, and SVD using a new technique for correction of main geometric attacks," *Optik - International Journal for Light and Electron Optics*, vol. 127, no. 2, pp. 964-972, 2016.

[7] I.A. Ansari, M. Pant, C.W. Ahn, "Robust and false positive free watermarking in IWT domain using SVD and ABC," *Engineering Applications of Artificial Intelligence*, vol. 49, pp. 114-125, 2016.

[8] N.M. Makbol, B.E. Khoo, T.H. Rassem, K. Loukhaoukha, "A new reliable optimized image watermarking scheme based on the integer wavelet transform and singular value decomposition for copyright protection," *Information Sciences*, vol. 417, pp. 381-400, 2017.

[9] N.M. Makbol, B.E. Khoo, "Robust blind image watermarking scheme based on Redundant Discrete Wavelet Transform and Singular Value Decomposition," *International Journal of Electronic and Communications* (AEÜ), vol. 67, no. 2, pp. 102-112, 2013.

[10] H.-C. Ling, R.C.-W. Phan, S.-H. Heng, "Comment on robust blind image watermarking scheme based on redundant discrete wavelet transform and singular value decomposition," *International Journal of Electronic and Communications* (AEÜ), vol. 67, no. 10, pp. 894-897, 2013.

[11] N.M. Makbol, B.E. Khoo, T.H. Rassem, "Block-based discrete wavelet transform-singular value decomposition image watermarking scheme using human visual system characteristics," *IET Image Processing*, vol. 10, no. 1, pp. 34-52, 2016.

[12] C.C. Lai, "An improved SVD-based watermarking scheme using human visual characteristics," *Optics Communications*, vol. 284, no. 4, pp. 938–944, 2011.

[13] T.D. Hien, Z. Nakao, Y.-W. Chen, "RDWT domain watermarking based on independent component analysis extraction," *Applied Soft Computing Technologies: The Challenge of Complexity. Advances in Soft Computing*, 2006, vol. 34, pp. 401-414.

[14] X.P. Zhang, K. Li, "Comments on an SVD-based watermarking scheme for protecting rightful ownership," *IEEE Trans. Multimedia*, vol. 7, no. 3, pp. 593-594, 2005.

[15] R. Rykaczewski, "Comments on An SVD-based watermarking scheme for protecting rightful ownership," *IEEE Trans. Multimedia*, vol. 9, no. 2, pp. 421-423, 2007.

[16] R. Liu, T. Tan, "An SVD-based watermarking scheme for protecting rightful ownership," *IEEE Trans. Multimedia*, vol. 4, no. 1, pp. 121-128, 2002.

[17] C.C. Lai, C.C. Tsai, "Digital image watermarking using discrete wavelet transform and singular value decomposition," *IEEE Trans. Instrum. Meas.*, vol. 59, no. 11, pp. 3060-3063, 2010.

[18] M. Khalili, "DCT-Arnold chaotic based watermarking using JPEG-YCbCr," *Optik - International Journal for Light and Electron Optics,* vol. 126, pp. 4367-4371, 2015.

[19] R. Keshavarzian, A. Aghagolzadeh, "ROI based robust and secure image watermarking using DWT and Arnold map," *International Journal of Electronic and Communications* (AEÜ), vol. 70, pp.278-288, 2016.

[20] M. Khalili, D. Asatryan, "Colour spaces effects on improved discrete wavelet transform-based digital image watermarking using Arnold transform map," *IET Signal Processing*, vol. 7, no. 3, pp. 177–187, 2013.

[21] R. Zhang, Y. Wang, "Scrambling image watermark algorithm based on DCT and HVS," *International Conference on Information Technology and Applications*, Nov. 2013, pp. 54–57.

[22] L. Gao, T. Gao, J. Zha, "Reversible watermarking in medical image using RDWT and sub-sample," *International Journal of Digital Crime and Forensics*, vol. 7, no. 4, pp. 1-18, 2015.

[23] C. Yim, A.C. Bovik, "Quality assessment of deblocked images," *IEEE Transactions on Image Processing*, vol. 20, no. 1, pp. 088-098, 2011.

[24] F. Ernawan, M. N. Kabir, J. M. Zain, "Bit allocation strategy based on Psychovisual threshold in image compression," *Multimedia Tools and Applications*, pp. 1-24, 2017.

[25] F. Ernawan, N. Kabir, K. Z. Zamli, "An Efficient Image Compression Technique Using Tchebichef Bit Allocation," *Optik - International Journal for Light and Electron Optics*, vol. 148, pp. 106-119, 2017.